

REMARKS

In the Office Action dated October 9, 2007 the Examiner has rejected the pending claims 1-16, 18-20, and 31-47. More specifically, the Examiner has rejected claims 1-9, 16, 19-20, 31-38, 41-45, and 47 under 35 USC 103(a) as being unpatentable over Tamaki et al. (US2003/0054796) in view of Dahan et al. (US2004/0123118); rejected claims 6 and 46 under 35 USC 103(a) over Tamaki in view of Dahan and in further view of Mahanti (US2002/0052824; rejected claims 10-11, and 39-40 under 35 USC 103(a) over Tamaki in view of Dahan and in further view of Kirkup (US20040142686); rejected claims 12-13 under 35 USC 103(a) over Tamaki in view of Dahan and in further view of Sakakura (JP2002209028); rejected claim 14 under 35 USC 103(a) over Tamaki in view of Dahan, Sakakura and in further view of Piazza (US2003/0061358); and rejected claim 15 under 35 USC 103(a) as being unpatentable over Tamaki in view of Dahan, Sakakura and in further view of Von Kaenel (US20040117358). Respectfully, the rejections are traversed below.

The Applicant notes that claims 1, 31, 35, 41, and 45 have been amended for clarification. Claims 16 and 18-20 have been canceled. Claims 48 and 49 have been added. Support for the amendments and the new claims can be found at least on page 8 lines 2-16. No new matter is added.

In the rejection that includes all of the independent claims 1, 31, 35, 41, 43, and 45 the Examiner again acknowledges that Tamaki et al. does not teach the use of trusted software, and states that this limitation is taught by Dahan in paragraph [0011]. The Examiner further states that it would have been obvious to apply the teachings of Dahan to Tamaki in order to "to improve security for the network". The Applicant disagrees with the Examiner.

Dahan discloses a security limitation of the prior art as "On a smart device enabled for a secure class of applications such as for m-commerce (mobile commerce) or ebanking (electronic banking), the user is asked to enter secret information such as a password on the keyboard or to sign messages displayed on the screen. When doing so, the user has no other choice then to fully

rely on the integrity of his device. However, there is no way for the user to detect that a hacker or a virus has defeated the security framework of his device" (par. [0009]). Dahan discloses "Thus, improvements in system security are needed" (par. [0010]), and further discloses:

"In general, and in a form of the present invention, a digital system is provided with a secure mode (3rd level of privilege) built in a non-invasive way on a processor system" (par. [0011]).

Dahan discloses that "In secure mode, the access to a physical user interface such as a keyboard or display are restricted to secure applications through trusted drivers. Otherwise, if a virus/hacker manages to download a forged driver on the smart device, then the user has no way to know that he cannot rely on his device" (par. [0022]). In addition, the "ROM is partitioned in two parts: a secure portion of the ROM that is protected by the secure bit and can only be accessed in secure mode; and a public portion of the ROM that is always accessible and contains the boot area" (par. [0054])"

Dahan discloses:

"Security signal 302 is asserted by security state machine (SSM) 300 under certain conditions. In secure mode, CPU 200 can only execute code that is stored in secure ROM 310 or secure SRAM 312. **Any attempt to run code stored outside of these trusted locations will generate a "security violation" by asserting signal 304 that will cause reset circuitry 306 to perform a global reset of the system,**" (emphasis added), (par. [0053]); and

"There is no software way to cause security signal 302 to be asserted or to modify the behavior of the state machine. The SSM is tightly coupled to an activation sequence that will be described in more detail with respect to FIG. 5," (emphasis added), (par. [0057]); and

"The purpose of the activation sequence is to take over the execution flow of the processor 200 and ensures that it cannot be preempted by any other non-trusted code. At some point during this part of the entry sequence, **security signal 302 is asserted to enter secure mode** and unlock access to secure resources (ROM, SRAM, peripheral devices, etc.)," (emphasis added), (par. [0058]).

Therefore, "The secure mode is entered when security signal 302 is asserted" and "In secure

mode, CPU 200 can only execute code that is stored in secure ROM 310 or secure SRAM 312” (par. [0053]). Further, the Applicant directs the Examiner to where as stated above Dahan discloses “There is no software way to cause security signal 302 to be asserted or to modify the behavior of the state machine.” The Applicant contends that the term “trusted software” as applied in Dahan merely relates to software that is intended to run **inside a trusted memory location** in a “secure mode.” Dahan is seen to relate to a method “for protecting sensitive information from access by non-trusted software” and for providing that “There can exist no possible flows by which non-trusted code can **either fool the hardware into entering secure Mode, or get trusted code to perform tasks it shouldn’t**,” (emphasis added), (paragraphs [0044] and [0045]).

As argued in at least two prior responses, yet not addressed by the Examiner, the Applicant contends that Dahan relates to securing a device by implementing a secure mode which prevents certain code from being executed on the device. The Applicant contends that Dahan clearly does not relate to trusted software comprising a certified unit of code and where at least the establishing a service provisioning relationship and the recording charging data for the relationship use the trusted software, as in claim 1.

Further, it is noted that Claim 1 has been amended for clarification to recite:

A method to provide a service for a user device with a service provider, comprising: establishing a service provisioning relationship between the user device and a bridging user device; providing a desired service for the user device with the service provider via the bridging user device; while providing the service, recording charging data for the service provisioning relationship between the user device and the bridging user device; and reporting the charging data from the bridging user device to the service provider, where at least the establishing and the recording use trusted software comprising a certified unit of code running on the user device and on the bridging user device, and where establishing includes at least one message comprising an indication of a requested charging metric is exchanged between the user device and the bridging user device.

Regarding Tamaki, the Applicant notes that Tamaki relates to a method for end users with wireless terminals to make connections to other wireless terminals via an ad hoc network of personal communications service provider repeater terminals without the mediation of base

stations in order to reduce costs, (Abstract and par. [0032]).

As cited by the Examiner Tamaki discloses:

“In order to receive low-priced communications service offered by the ad hoc network of terminals with repeater function owned by personal communications service providers, **the end users and personal communications service providers take the registration procedure for personal communications service provider and make a contract to pay a monthly fee based on the flat rate system to the communications service provider**. Now, the end users and personal communications service providers can selectively receive the communications service from the communications service provider, the information service from the information service provider and the low-priced repeater (data transfer) service from the personal communications service providers,” (emphasis added), (par. [0035]).

The Applicant notes that Tamaki appears to disclose that the end users and the personal communications service provider each make a contract with the communications service provider to pay “a monthly fee based on the flat rate system” for the service. The Applicant submits that here Tamaki is not seen to disclose or suggest **establishing a service provisioning relationship between the user device and a bridging user device**, as in claim 1.

Further, referring to Figure 14, Tamaki discloses:

“First, the request node broadcasts a route request message (packet) and waits for a route reply packet,” (par. [0045]); and

“When the personal communications service provider terminal receives the route request packet, [...] If the destination address is found in the routing table and the idle time is valid or within the limit, it checks whether or not there is a valid route to the destination node which satisfies the requested link speed. If so, it sends back the route reply packet to the request node; **if not, it transfers the route request packet**,” (emphasis added), (par. [0046]); and

“As the destination node receives the route request packet, [...] it sends back the route reply packet to the route whose average throughput satisfies the requested link speed. Then, the route reply message traces the route to the request node in the reverse order to reach it; **thus a communication link for the ad hoc network**

is established," (emphasis added), (par. [0047]).

Thus, it can be seen that the personal communications service provider terminal in Tamaki appears merely to forward route request packets from the request node to the destination node after which a route reply message from the destination node traces back to the request node to establish the communication link.

The Applicant contends that Tamaki does not disclose or suggest that a message is exchanged between a user device and a bridging user device **which indicates a requested charging metric** as in claim 1. The Applicant contends that Tamaki clearly does not disclose or suggest **"establishing a service provisioning relationship between the user device and a bridging user device;** providing a desired service for the user device with the service provider via the bridging user device [...] where at least the establishing and the recording use trusted software comprising a certified unit of code running on the user device and on the bridging user device, and **where establishing includes at least one message comprising an indication of a requested charging metric is exchanged between the user device and the bridging user device,"** as in claim 1.

For at least the reasons stated, the Applicant contends that the references cited can not be seen to disclose or suggest claim 1. The Applicant contends that without expressly or impliedly admitting that the proposed combination is suggested, clearly the proposed combination would not disclose or render obvious at least the subject matter that is highlighted above for claim 1.

In addition, for at least the reasons stated above the references cited can not be seen to disclose or suggest, as claim 16 recites in part:

"where said user device, said bridging user device and said service provider execute computer code **to establish a service provisioning relationship between said user device and said bridging user device**"..."**to record charging data for the service provisioning relationship** between said user device and said bridging user device"..."where said computer code comprises trusted software comprising a certified unit of code running on said user device and on

said bridging user device.".

In addition, for at least the reasons stated above the references cited can not be seen to disclose or suggest, as claim 31 recites in part:

"where said computer code **comprises trusted software comprising a certified unit of code running on said mobile device and on said another device, and **where to establish the service provisioning relationship includes at least one message comprising an indication of a requested charging metric is exchanged between the mobile device and the another device...**"**

In addition, for at least the reasons stated above the references cited can not be seen to disclose or suggest, as claim 35 recites in part:

"said computer code **comprising trusted software comprising a certified unit of code running on said mobile device and on said another device, **where to establish the service provisioning relationship includes at least one message comprising an indication of a requested charging metric is exchanged between the mobile device and the another device...**"**

In addition, for at least the reasons stated above the references cited can not be seen to disclose or suggest, as claim 41 recites in part:

"..where said data processor **operates under control of trusted software comprising a certified unit of code stored in said mobile terminal and in said device, **where to establish the service provisioning relationship includes at least one message comprising an indication of a requested charging metric is exchanged between the mobile terminal and the device...**"**

In addition, for at least the reasons stated above the references cited do not disclose or suggest, as claim 43 recites:

"where said data processor is further operable to exchange at least one message comprising an indication of a requested charging metric between the mobile terminal and the device to establish the service provisioning relationship".

In addition, for at least the reasons stated above the references cited can not be seen to disclose or suggest, as claim 45 recites in part:

“establishing a service provisioning relationship with a user device; providing a desired service for the user device with a service provider; while providing the service, recording charging data for the service provisioning relationship; [...] where at least the establishing and the recording use trusted software comprising a certified unit of code running on the user device and on the bridging user device, and where establishing includes at least one message comprising an indication of a requested charging metric is exchanged between the user device and the bridging user device.”

Further, for at least the reasons stated the Applicant notes that the references cited can not be seen to disclose or suggest at least where claim 48, which depends from claim 1, recites in part **“where the at least one message exchanged between the user device and the bridging user device further comprises a determination of a usage cost for the requested charging metric.”**

Further, for at least the reasons stated the Applicant notes that the references cited can not be seen to disclose or suggest at least where claim 49, which depends from claim 45, recites in part **“where the at least one message exchanged between the user device and the bridging user device further comprises a determination of a usage cost for the requested charging metric.”**

In that the references cited can not be seen to disclose or suggest the subject matter found in claims 1, 16, 31, 35, 41, 43, 45, 48, and 49, the Applicant contends all the claims 1, 16, 31, 35, 41, 43, 45, 48, and 49 should be allowed.

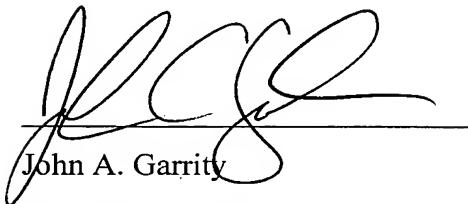
Further, for at least the reason that claims 2-15 and 46, 18-20, 32-34, 36-40, 42, and 44 and 47 depend from claims 1, 16, 31, 35, 41, and 43, respectively, all the claims 1-16, 18-20, and 31-49 are seen to be allowable over the references cited.

S.N.: 10/792,181
Art Unit: 2617

The Applicant again provides notice that the indicated allowability of the claims for these reasons alone should not be construed as an acknowledgment that the Applicant is in agreement with the Examiner's other reasons for rejecting the claims based variously on Tamaki and the other cited documents.

The Examiner is respectfully requested to reconsider and remove the rejections of the claims, and to allow all of the pending claims 1-16, 18-20, and 31-49 as now presented for examination. An early notification of the allowability of claims 1-16, 18-20, and 31-49 is earnestly solicited.

Respectfully submitted:



John A. Garrity

Reg. No.: 60,470

Customer No.: 29683

HARRINGTON & SMITH, PC

4 Research Drive

Shelton, CT 06484-6212

Telephone: (203)925-9400

Facsimile: (203)944-0245

email: jgarrity@hspatent.com



Date

S.N.: 10/792,181
Art Unit: 2617



CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. BOX 1450, Alexandria, VA 22313-1450.

1/7/2008

Clairie L. Man

Date

Name of Person Making Deposit